CHAPTER

2

CORPORATE COMPONENTS TO SECURITY PLANNING

After reading this chapter and completing the exercises you will be able to:

- Identify the business model for a corporation and how the model will affect the corporate security plan.
- Identify the corporate organizational structure and how the structure will affect the corporate security plan.
- Identify the corporate goals and strategies and how these components will affect the corporate security plan.
- Identify the corporate IT administrative structure and how this structure will affect the corporate security plan.
- Identify the current IT infrastructure and how the infrastructure will affect the corporate security plan.
- Identify the current IT security plan and how this plan will affect the development of a new security plan.

Now that you have an understanding of the security threats that an organization faces, you are ready to move on to the next step in the security design process. That next step is to collect a great deal of information about the organization that you are working with. Designing a corporate security policy can never be done in isolation from the rest of the corporate environment. If you design the plan without consulting the stakeholders in the security plan, you may not have their support when you are ready to implement the plan. Part of the reason for this might be a corporate history or corporate culture. Every organization has certain procedures for doing things, and sometimes there is a great deal of resistance to any kind of change. Every corporation has a decision-making process, and proposals that follow the correct process may be approved, while equally good proposals that don't follow the procedure may be rejected.

In addition to the sometimes clouded corporate culture issues, you also have to take into consideration the current corporate structure, both from a business perspective and from an IT perspective. An essential part of planning the security policy is to collect information about the organization. This information includes details on the corporate goals, business practices, products and processes, and how all of these components are expected to change during the time that the security policy remains in effect. As well, you need to gather information on the IT infrastructure and the current security plan. You need to collect basic information about the company locations, the location of the corporate information and services, the connections between corporate locations, the connections to the Internet, and so on. Even if your security plan is going to result in a drastic departure from the current way of doing things, you must understand the current structure before you can begin to plan.

The amount of information that you need to collect depends to a great extent on the scope of the security project that you are working on. If you are designing a security solution for one small office in a large corporation, most of the information you gather will focus only on that office. If you are designing just the firewall or demilitarized zone (DMZ) configuration for the corporation, you might need only the Internet access information. Ideally, however, each small part of the security policy will be part of a much larger whole, which means that you need to collect information about the entire organization. In this chapter (and throughout the book) the assumption is made that you have been given the responsibility of designing a security solution for an entire company, which means that you have to collect information about the entire company.

Identifying Business Models

In most cases, when you collect information about a corporation, it is easier to start from the higher corporate levels and work your way down to the lower, more detailed technical information. By looking at the top-level business model and business processes, you can begin to understand the corporate culture and what the business goals are for the organization. If you begin by looking at all the details of how the company is organized, or why things are done in a certain way, you may have a hard time figuring out the big picture.

A business model is a way to try to understand a company by looking at it from different perspectives. There are several different ways to determine a business model for a corporation. The components of a business model include the following:

- Ownership and control
- Products and services
- Corporate geographic scope
- Business processes
- Corporate management models
- Business relationships with other corporations

Ownership and Control

A corporation's ownership structure can have a great deal of influence on the corporate IT structure, including the security model. There are several different models for corporate ownership. Most large corporations are publicly traded corporations. These corporations are owned by stockholders, who elect a board of directors. The board of directors is responsible for the overall management of the company and sets top-level direction for the corporation. The board is also responsible for hiring the executive officer(s), who actually manage the company on behalf of the board of directors. The executive officers then hire the additional executives to help run the company. Figure 2.1 illustrates the corporate structure for most large corporations.

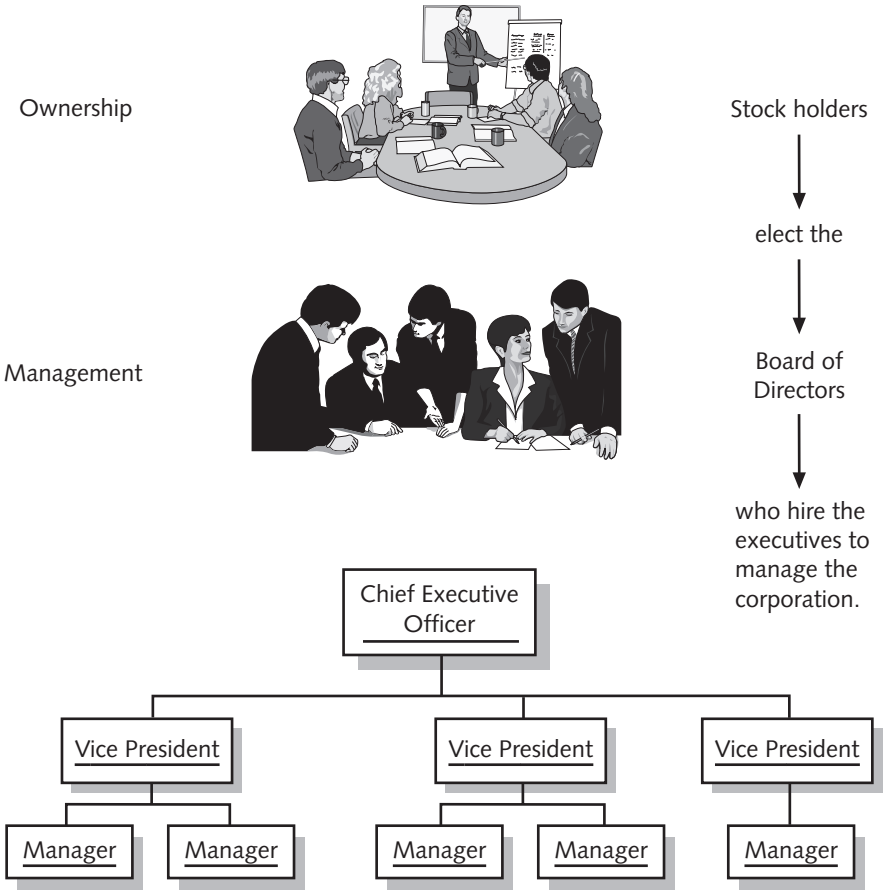

Figure 2-1 Corporate structure for a publicly traded company

A publicly traded corporation is usually driven by the desire for maximum profits (this is obviously not unique to publicly traded corporations). The stockholders who invest in a corporation do so with the goal of getting a return on their investment. As the representatives for the stockholders, the members of the board of directors have the responsibility to make sure that the company makes a profit. Ultimately this pressure to make a profit filters down to the chief executive officer (CEO), whose success or failure (and ultimately, job security) is determined largely by the return on investment to the stockholders. The rate of return on investment can also have a great impact on the viability of the corporation. If the corporation is making a healthy profit, the stock prices go up, and the corporation may consider expansion. If the corporation is losing money, the stockholders may off-load their stocks and the stock prices may begin to drop. Often large corporations respond to this scenario by cutting costs throughout the organization. If a board of directors sees that the corporation is losing money, they may order a 10% reduction in costs, and the CEO must determine how to achieve this goal.

The ownership structure of a publicly owned corporation can have a great effect on the corporate IT, including any security plan. In large, established companies that have a long history of making profits, the stock prices may be very stable, and, as a result, the possibility for effective long-term planning exists. If a company has done well for many years, the board of directors will probably be confident that the success will continue, and one or two years of lower profits are not likely to result in large changes in corporate direction. In this environment, the IT infrastructure probably also has the luxury of doing long-range planning with considerable confidence that the planned projects will be completed.

In a more volatile company, this situation can change drastically. If the company is doing very well one year, there may be considerable freedom to spend money on new projects and to research new technologies. In a good year, the IT department may be given the directive to develop a comprehensive security plan, almost without regard for cost. However, if the profits decrease dramatically over the next year or two, the IT department may be forced to stop all new spending, or even to decrease the money spent on IT. The comprehensive proactive security plan may be put aside and replaced with a reactive security plan that deals with problems only after they happen.

As you begin to develop the security plan, the pressure for a publicly traded company to make money can affect your planning. If the company is stable and profitable, the chances are very good that a long-term comprehensive plan will be accepted. If the corporation is less stable, and there is a great deal of pressure to maximize the profit every year, you will probably need to look at projects that can be planned and implemented in a shorter period of time, because you may not get the long-term funding needed.

Regardless of the ownership structure of a corporation, one important determinant of whether the planning and implementation of the security plan will succeed is the amount of support you receive from the executive level in the company. Most large organizations appoint a project sponsor to oversee the implementation of IT projects. This person is responsible for the overall direction of the project, as well as the budget. If this person is strongly committed to the success of the project and has the executive power to come up with the budget, then the project has a good chance of succeeding. If the project sponsor does not strongly support the project, or cannot guarantee the budget required for the project, then that project may get cut when the times get tough. In addition to being responsible for budget concerns, an influential project sponsor can also be essential in dealing with resistance within the company.

Another possible ownership model for a large company is private ownership by a single individual or a small group of individuals. The goal of a privately owned corporation is also to make a profit for the owners, so in many ways the corporate culture may be very similar to a publicly owned corporation. In most cases, the owners of the corporation act as the board of directors, setting overall direction and hiring a CEO to actually run the company. In other cases, the owner or owners take a more active role in the day-to-day management of the company.

From an IT planning perspective, the only thing that changes in a privately owned corporation is that the high-level corporate direction is usually set by a smaller group of people. If a corporation has a single owner, that owner will obviously be able to completely control the direction of the corporation. The success or failure of the IT projects then becomes more dependent on the support of the owner. If the owner sees the IT infrastructure as being essential for the success of the corporation, then the project will get the funding and support required.

Another common ownership model for a large organization is that of a wholly-owned subsidiary where a corporation may be owned by a much larger corporation. In some cases, the subsidiary may be run as a fairly independent business unit within the larger corporation, where all of the decisions affecting the subsidiary are made by the subsidiary's executives. In this case, working for the subsidiary is not much different than working for a publicly traded corporation. As long as the subsidiary shows a profit for the parent company, it can run fairly independently. If the subsidiary begins to lose money, the parent company, which has to show a profit for its shareholders, may begin to impose direction on the subsidiary to try to show a profit.

Other subsidiary companies are much less independent and may have to deal with much more direct management from the parent company. In this scenario, the executives of the subsidiary may have very little direct decision-making power and important concerns may have to be dealt with at the parent company level. This scenario can be very frustrating for the IT management. The IT staff may come up with some excellent projects for the IT infrastructure, but when the time comes to get the project approved, it

may be turned down by the parent company, sometimes for excellent business reasons, sometimes for budgetary reasons, and sometimes because the parent company is going in a different direction with its IT planning. This can be very frustrating for the IT staff of the subsidiary company, who might be responding to local conditions that are not understood by the parent company.

There are a number of other ownership scenarios that you might have to deal with, but these are the major categories. One other situation is that of an independently owned company that has another company as its only or primary customer. In this situation, the company, although independently owned, may have to respond to the requirements of the customer. For example, if the customer decides that it will only do business with companies that provide certain information on the Internet, or with companies that use a particular type of messaging system because they want to replicate some public folder information, then the company has to respond and provide this service. In this case, the company may be forced into adopting a technology that it might not otherwise implement.

In a large corporation, the owners of the company may seem far removed from the actual work of the IT staff. However, the owners can directly affect the work that you do. The owners may have strong beliefs on the business benefits of technology and the future profitability of implementing technology, even at the cost of short-term profits. In this situation, the IT staff can be quite creative in long-term planning with the assurance that well-planned projects that answer business requirements will be approved and implemented. If the owners do not have this same commitment to technology, even well-planned projects that may have long-term business benefits may be cancelled simply because of the cost.

IT managers sometimes have a hard time dealing with the business managers in an organization because the focus of the two groups is so different. IT managers understand technical needs and how technology works, and business managers understand the business requirements and how the business process works. What is often missing is an understanding on both sides of how to work together. IT managers need to understand how the business works, so that they can provide technical solutions according to business requirements, and business managers need to understand technology so that they can see which of their business needs can be addressed with technical solutions.

Products and Services

Another way to look at a corporation is to focus on what the corporation produces, and how the products and services are sold and delivered to the company's customers. What a company does, and how it does this, can have significant implications for the IT infrastructure. For example, a manufacturing company where 75% of the employees work on an assembly line will have very different technology requirements than a financial company where the employees need immediate access to stock market information.

To understand what the corporation does, you need to understand what products or services the corporation produces and sells. The corporation may produce a product such as raw materials like iron ore or coal, or a highly manufactured product such as stereo systems. The product may be a single component like a microchip that will be sold to another company, or a complete product like a cell phone that is ready to be sold to consumers.

In today's economy, many companies sell services rather than produce products. An insurance company sells life insurance or home insurance as a service to its customers. A technical consulting firm sells its consulting services to other companies. A travel agent sells a service. The service provided can be very different in different corporations, or one corporation may sell many different services. An insurance company may offer a wide variety of insurance policies in an effort to provide the service to as many groups of people as possible. A technical consulting firm may employ highly skilled people who provide a very specialized service to only a small group of companies.

As you gather information about the products and services that a company sells, you should also gather information about how the company sells its products. There are many ways to sell products or services. Some companies, like retail stores, may depend on the customer coming into the store and choosing the product they want. Some companies may do all of their business on the Internet, or through a mail-order process, and the company may never actually see any customers. Other companies depend on a team of sales people or agents to go where the customers are in order to sell the products. Many companies use a wide variety of methods to sell their products. A financial services company may have an office for walk-in customers, an Internet site for online customers, and hundreds of agents to sell their services to potential customers.

In addition to determining how a company sells its goods and services, you should also understand who the corporation's customers are. A retail store will try to appeal to as many customers as possible, often with the goal of making hundreds of small sales every day. Customers of a company manufacturing transit buses are primarily cities who need to buy buses for their transit system. The bus manufacturing company might have to spend months and go through an intensive process to make a single sale, and may make only a dozen sales in a year. A company that manufactures automobile components may have only a single customer—all of the products that the company produces may be sold to the company that actually builds the car.

In addition to the questions that you ask about the current products, you also need to ask questions about the future of the products that the company makes. What is the proposed life cycle of the products or services that the company currently provides? What new products and services are being developed? What is the process that a new product goes through as it moves from potential product, to research and development, to product approval, to manufacturing? Your security plan should meet the corporate requirements for several years to come, so you need to look forward to see what new products and services are being developed, and how these will affect the security requirements.

As Figure 2-2 illustrates, there are many questions that you need to ask about a company's products and services. The answers to these questions will greatly affect your security design, as well as the entire IT infrastructure. A small retail store may have several computers in the office and computer terminals for the cashiers. The store may have no connection to the Internet, and only a dial-up connection to a bank for credit card and debit card transactions. The security requirements for this store will be much different than the security requirements for a financial services company that provides online banking for its customers, and whose servers store financial information worth billions of dollars. A company providing online sales that require credit card information from its customers has much different security requirements from a manufacturing firm whose only Internet presence is an informational web site hosted by an Internet Service Provider (ISP). A software development company writing the code for the next version of its software has very different security requirements than a company that builds houses.

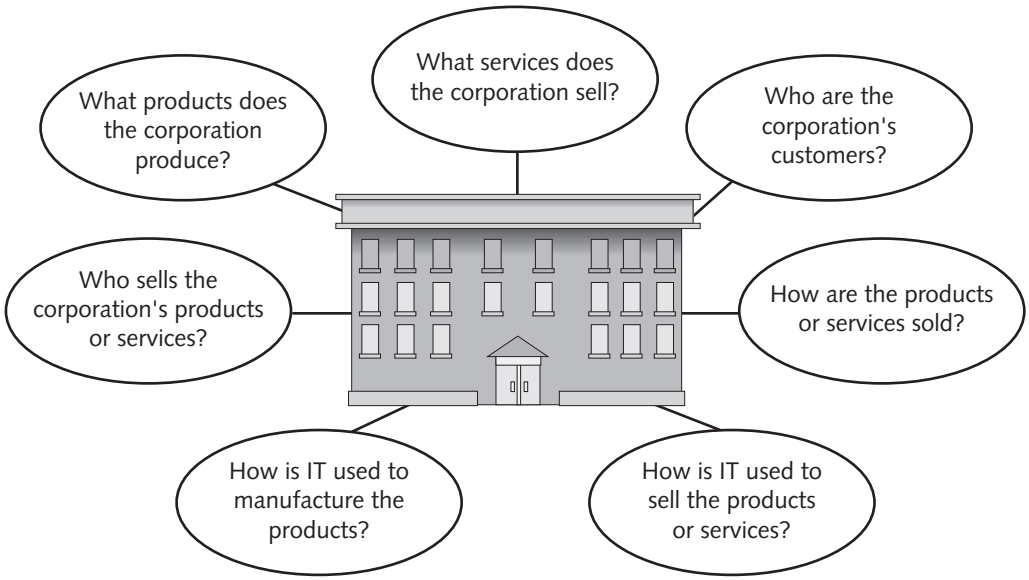

Figure 2-2 Examining the products and services a corporation sells

Business Processes

Understanding what the corporation produces and sells is also important in mapping out the business processes that a corporation uses to get its work done. This will help you to make sure that your security plan is the most appropriate for your company. A business process is simply a mapping out of how the company does its work. The business process can be very complicated and include many different components. Figure 2-3 illustrates a simplified possible business process that a bus manufacturing company might go through from the time that it first contacts a potential customer until it delivers the buses to the customer. Figure 2-4 illustrates some of the possible business processes that an insurance company might have.

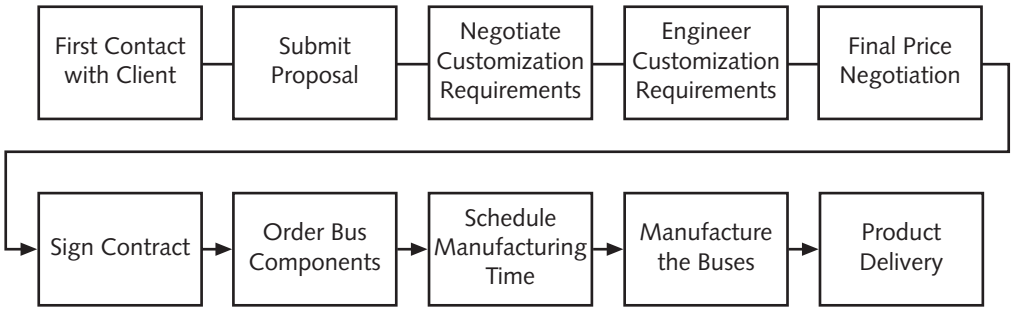

Figure 2-3 A business process at a bus manufacturing company

These examples are obviously very simplistic. The complete diagram of the business process for a large corporation can cover an entire wall of a large room. Understanding the business processes has always been important to business analysts, who work with software architects to build customized applications for corporations. The business analyst has to know exactly what happens at each step of the business process so that the application that is used during that part of the business process can meet the business needs. As a security expert, you will not need to know the business processes down to that level of detail, but you will need to understand the overall processes. At each step in the process you need to know how the IT infrastructure is used and what the security implications are. For example, if the insurance company lawyers are sending confidential corporate documents by e-mail, how can you ensure that the documents cannot be read or tampered with while they move between servers?

In addition to the actual processes that a corporation uses to get its work done, you should also understand several other business process issues. One of these is the communication and information flow in the company. How does information get moved around in the company? In many companies these communication processes have changed considerably in the last several years. Three years ago, most companies depended on paper memos, phone calls and face-to-face meetings to communicate business information. Now many executives may get only a couple of messages a week in the paper inbox, but hundreds of messages a week in their e-mail messaging inbox. Almost all executives now carry cell phones or other mobile communication devices, which means that their physical location is much less important to getting work done. Video conferencing has replaced traveling to meetings in some corporations. Understanding how information is moved throughout the corporation is an essential first step towards protecting that information.

Almost every corporation has both public and private information. The public information is made available to everyone who wants it, usually through corporate documents or a web site. Private information is usually accessible to only employees of the company, or most often, only some of the employees. Many companies also have other categories of information. They may make some information available to customers, but not to the general public. A partner organization may get access to some confidential information, but must be prevented from getting access to other information.

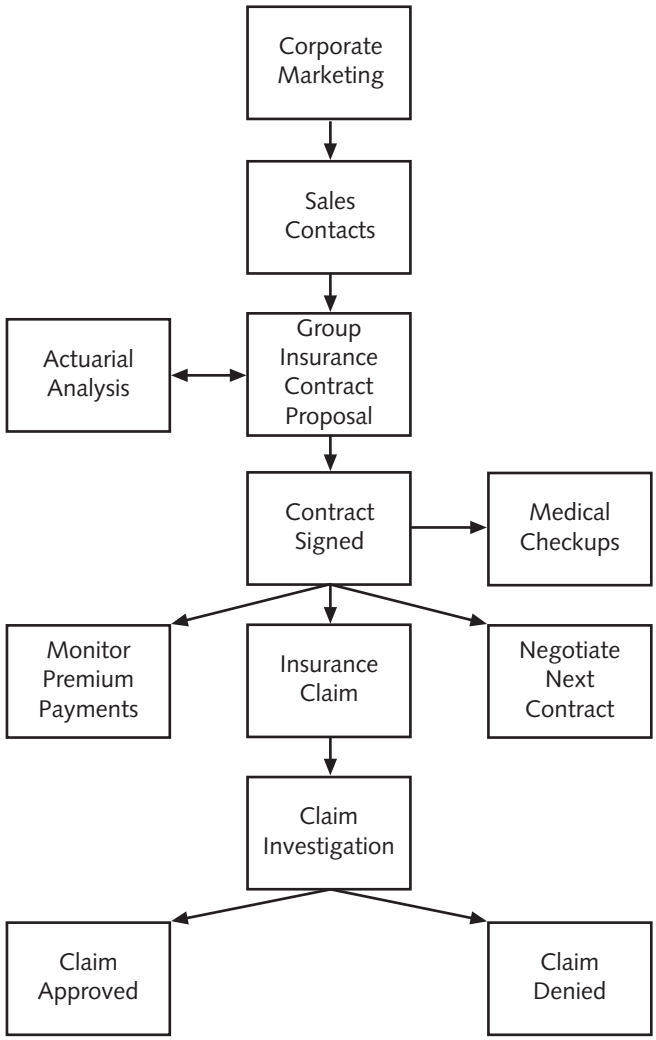

Figure 2-4 A business process at an insurance company

As the security expert, you need to understand what types of information your corporation has, and who should have access to that information. This can be very useful in making sure that you are using the appropriate method of communicating the information you want to send. More importantly, you are also responsible for maintaining the security of the information as it flows through the IT infrastructure. The executives in the company may be using a share on the server to store confidential business information that three years ago was stored in a locked vault. They expect that their information is as secure as it

was in the vault. To develop the security plan concerning private and public information, you need to understand clearly what information is included in each category, and how the decisions are made concerning into which category the information fits.

Another crucial component to the business process that you need to understand is the decision-making process at the corporation. Often businesses have a formal hierarchical structure from the CEO down to the front-line workers. In some companies, the decision-making process follows this hierarchical model. In this model, all of the decisions are made at the top level and implemented at the lower levels. In other corporations the decision-making process is much more fluid. People further down the corporate structure may have significant decision-making power. Sometimes the real decision-making power rests with an informal group who may not exactly fit into the corporate hierarchy.

As you plan the security model for your organization, you need to understand the decision-making procedures to ensure that your plan will be implemented. If you can clearly identify where the effective decisions are made in the corporation, then you can focus on these people to get approval for your project. For example, one of the items in your security plan should be how to deal with users on the network who use the Internet inappropriately. Who will decide what inappropriate Internet use is, and who will enforce the policy? In most cases, the security policy is only useful in detecting the offender, and someone else will be responsible for enforcing the policy. Another item you should include in the security plan is a response plan if your web server is under a denial-of-service (DoS) attack. Your security plan needs to clearly identify who has the authority to make important decisions; such as whether to disconnect the Web server from the Internet in response to a Web server attack.

Corporate Geographic Scope

Before you create your security plan, you need to understand the geographic scope of the organization. The security requirements for a corporation with locations throughout the world will be very different from an organization with just one office in a single city.

Many of the large corporations today are international organizations. These companies have locations in many countries around the world. The head office for the corporation may be on one continent, with manufacturing, sales, or subsidiary offices in other cities throughout the world. Creating a security plan for an international organization is a difficult task because of the number of issues that you will face. Part of the reason for this is simply the difficulty of managing an IT infrastructure for an international organization. An organization with locations around the world will have to deal with multiple languages. If the corporate users are located around the world, you do not have the standard downtime at night when you can do server maintenance or backups. The speed and reliability of WAN links can add complexity to the task of managing the network. A large organization may have several domains throughout the world, which can complicate something as simple as assigning share permissions.

International organizations also face a variety of challenges in designing the security infrastructure. For example, until recently, American companies were not allowed to export applications using 128-bit encryption outside of North America. This law has been relaxed, but when you are designing a security plan for an international company, you will still be faced with a variety of laws and requirements in the different countries. Companies with multiple locations will have WAN connections that must be secured, as well as multiple access points to the Internet.

Companies that are national in scope usually have less complex security issues. The laws that apply to your security options are more uniform. As well, you are likely to have fewer WAN connections to be concerned about, and you may have only a single access point to the Internet.

Regional companies can be identified as companies that are located in only one region or even in just one city. These companies may have only a single location, or multiple locations close together. Again, the smaller the company, the less security requirements it will have. A small company may have no WAN connections to manage and only one Internet access point. A small organization is likely to have only one domain, which means that managing security groups and permissions is not too complicated. One of the biggest issues facing a small organization is the lack of a person dedicated to managing the security of the IT infrastructure. Small companies often have one or two network administrators who have to manage all aspects of the network, including security. This lack of specialization can lead to errors in the security configuration. Small offices are sometimes careless about the way security is designed. In some offices, everyone knows all of the passwords, or half the people in the office know the administrator password. If you do design the security plan for a small office, the focus usually has to be on keeping it as simple as possible, while still providing the needed security.

In addition to office locations, you also need to know where the users of the IT infrastructure are actually located. A company may have only one or two locations, but it may also have several people who travel frequently and who want to be able to access the network from a hotel room or an airport. Or a national company may have numerous people across the country, in small offices or home offices, who need continuous access to the network. As you collect the information required to create your security plan, you need to keep this in mind.

The detailed information on what types of information you need to gather comes later in the section that analyzes the current IT infrastructure.

Corporate Management Model

Another important component of a business model is the corporate management model that is currently in place. Every organization has its own unique management model, but generally, it will fall under one of four categories. Some companies are managed

according to a very hierarchical and centralized model where all the planning is done at the top of the organization and the lower levels of the organization are expected to follow only directives from the top. At the other extreme are very non-hierarchical and decentralized models where there are very few layers of bureaucracy between the top and the bottom of the organization, and where a great deal of the decision-making authority rests with the front-line workers for the organization. A third model that is employed by some corporations is a team approach where people are grouped together based on a project or product that they are working on, and each team is allowed to operate almost autonomously. The fourth model is a hybrid model, adopting components from each of the other three models.

Most large corporations have traditionally been highly centralized and hierarchical. In these companies, the CEO or the top executives make all of the important decisions. The decision is then passed down to the lower levels of the corporation, where the policies are implemented. In some cases, the hierarchical structure can also be quite authoritarian, where initiative at lower levels is not recognized or encouraged. Other organizations may be quite hierarchical, but still encourage everyone in the organization to make suggestions on how the corporation can be run more effectively. Often large organizations fall into this category, where all of the important decisions are made at the head office, and the branch offices are expected to simply follow the directives. Small companies might not be as hierarchical, but might be just as centralized. In a small company, it is not uncommon to have the founder or owner of the company develop a very centralized management structure. The owner may want to make all decisions and may find it very hard to delegate management tasks.

Some corporations have adopted a much more decentralized approach to managing the company. In a decentralized model, the decision-making authority is delegated to a broad group of people rather than centralized in a small group. Sometimes this type of structure is the result of a corporate merger, where several formerly autonomous companies have merged to form one company. In this environment, the former companies may maintain a great deal of their autonomy in the larger organization. Other corporations have deliberately created a decentralized model by creating separate business units within the company and transferring a great deal of decision making to the business units. Companies that have several geographic locations may give each location considerable leeway in developing their own business direction.

A third model is a team approach to company management. In this model, the corporation is organized around projects or products. For example, in an insurance company, all of the people working on group insurance may make up a semi-autonomous group. Or the teams may be grouped around projects—all of the people involved in developing a new piece of software may form a team that includes software architects, programmers, business analysts, and marketing and sales personnel. In this environment the team can operate with considerable autonomy within its area of responsibility, and may have little overlap with any other teams in the company.

The fourth approach to company management is the most prevalent because it is a combination of the other three. Most corporations have at least some components of the three management styles. The executive office may by quite hierarchical and centralized and set the direction for the entire company. However, under the executive level, there may be multiple business units with considerable autonomy, as long as they support the overall direction set by the executives. Within each business unit, there may be another hierarchical structure, with some of the people organized into project teams for short-term or long-term projects.

As you begin to create your security plan, you need to determine the corporate management structure. Usually the first step towards beginning this research is to obtain a copy of the corporate organization chart. The organization chart can be extremely useful in identifying the management structure, as well as for determining the people that you need to talk to if you want to get answers to some of your questions. The organization chart should not be your only source of information, however. One reason for this is that the chart can be quite misleading. Some companies have an organization chart that appears very hierarchical and centralized, but in reality a great deal of autonomy may have been granted to teams at the bottom of the hierarchy. Organization charts are also notorious for rarely being up-to-date. Many corporations seem to reorganize departments and roles on a fairly regular basis, and the organization chart may be a couple of reorganizations behind. So although the organization chart is a good place to start your research on the corporate management structure, you will also need to interview people within the organization to get an accurate perception of what really happens.

The corporate management model will have a great deal of influence on what your corporate security plan will look like. A hierarchical, centralized corporation will likely be looking for a security policy that is also highly centralized. In a decentralized corporation, each business unit or geographic location may be free to develop its own security plan with very little direction from the head office. This can be advantageous for each business unit as it can develop a security plan that responds to local conditions and business requirements. The disadvantage of a decentralized security model is that the corporation may find itself supporting a wide variety of security components. For example, if each business unit can choose its own firewall, the administrators may find themselves supporting multiple, different firewalls. If each business unit controls its own naming convention for users and groups, managing permissions on information shared between business units may be very difficult. In a worst-case scenario, different business units may wind up developing security policies that are incompatible with each other. For example, if one business unit decides to use IPSec to encrypt all SMTP mail, while another business unit decides to use Secure MIME, the two departments will have a very difficult time exchanging e-mail messages with each other. Because of these difficulties, it is usually best if the central decision-making group imposes at least some general guidelines as part of the security plan.

Relationships with Other Organizations

A final component to the business model is the corporation's relationship with other organizations. These other organizations may be vendors, partners, or customers. Because the corporation must have a close relationship with each of these organizations, your security plan must take these relationships into account.

The first step in collecting information about the interorganizational relationships is to determine which companies are involved and what the nature of the relationship is. Essentially there are three types of relationships: vendor, customer, or partner. In a vendor relationship, the other organization provides a product or service for your organization. If the other organization is a customer, you are providing a product or service for that organization. Many corporations have also formed partner relationships with other corporations. Sometimes these partnerships are formed for the duration of a project, in which the two companies are working together on a single project. Other partner relationships have a much longer lifespan, and may involve many departments or projects.

Once you understand the relationships that your corporation is involved in, the next step is to understand what types of information have to be shared with each of the partner organizations. In most cases, the information that you share with other companies may not have any security implications; however, sometimes the security issues may be very important. In a relationship with a vendor organization, you may be providing the other company with technical specifications for the products that you are buying. If the other organization is providing a service (for example, if the organization is an IT security company designing a security plan for your organization), you may be providing the company with confidential security information. In a customer relationship, you may be providing the other company with confidential data about the product you have sold to the company. In an effort to make a sale, you may even be providing the other company with confidential information about future products. If your company is working with another company on a large project, your company may share quite private corporate information with the partner organization.

Before your organization shares confidential information with another organization, you should get at least a basic understanding of the security model of the partner organization. You may have implemented an excellent security policy and be quite confident that no one can get inappropriate access to information on your network, but if you share this confidential information with another organization, you are also dependent on that organization to keep the information secure. Your efforts to protect your information are wasted if the other organization doesn't protect it after they get access to the information. When you design your security plan, you need to take into account the security policies of all the companies that your organization shares confidential information with. If you don't think that another organization is protecting the data that you make available to them, then you need to build as many safeguards as possible into your security plan to protect your data.

Identifying Corporate Strategies and Goals

As described in the previous section, you need to identify a corporation's business model as a first step in creating your security plan. A business model is a description of how the company does its business, what processes it goes through, what restraints control how the business operates, and what forces are moving the corporation forward. Another important part of the business that you need to understand if you want to design the ideal security solution is where the business is going. In this section, we will examine this question—where is this company going and how is it planning on getting there?

Corporate Vision and Goals

As a corporation looks to the future and tries to decide where it wants to go, the first thing it has to do is define a vision, and then decide on the steps it will take to implement the vision. A corporation's vision and goals should drive all of the activity in the organization. The corporate vision provides the answer to the question, "Why are we doing this?" The vision defines why the company is in business. Once the corporate vision and goals are understood throughout the organization, they provide a clear measuring stick against which all decisions and actions can be measured. In most corporations, the board of directors and executives develop this vision. The upper management then has the task of articulating this vision to all employees of the corporation. After the corporation has defined the vision, the next step is to define the corporate goals. If the vision defines where a company is going, then the goals are practical steps that define how the corporation is going to achieve the vision.

It's essential to have a clear understanding of the corporate vision and goals when beginning a project like designing a security plan. The corporate vision and goals define where the corporation is going, and the security plan has to be responsive to that direction. Everyone involved in the project must understand the vision and be committed to achieving it.

Before you begin the process of designing the security plan, you need to be able to answer some basic questions:

- What is the corporate vision?
- What are the corporate goals?
- How is the corporation planning to achieve these goals?

Once you understand the answers to these questions, the process can continue. However, without a clear understanding of the corporate vision and goals, you will not be able to articulate how your security plan can help the corporation achieve its goals. In other words, until you know where you want to go, you can't really determine the best way to get there.

Growth Strategies

An essential part of the corporate vision and goals is the corporation's plan for growth, as well as the strategies for achieving that growth. Almost every corporation plans to grow, and you must take this planned growth into account when developing your security plan.

On a very simplistic level, there are three ways for a company to grow. The first way, which has become very popular, is for a company to grow through mergers and acquisitions. In this scenario, a company grows by buying other companies or merging the ownership of two or more companies. Sometimes the acquisition involves buying another company that is similar to the parent company. For example, an insurance company might buy up a smaller insurance company. In other cases, the acquisition can be something completely different. An insurance company may buy a real estate management company in order to diversify its business. An acquisition or merger can be either the most difficult or the easiest type of growth when seen from an IT perspective. If each company remains quite distinct, and there is little requirement for any merging of the two IT departments or of merging the management of the two networks, then the amalgamation of the companies may have little impact. However, if the two companies are going to be working very closely together, and most of the data and services must now be shared between users in both companies, then the amalgamation can be very difficult to implement. The two companies may have completely different security issues and policies, and finding a way to come up with one security policy for the two companies can be technically challenging, as well as politically difficult.

A second way that a corporation can grow is to just do more of what it is currently doing. A bus manufacturing company may decide to expand its operation and open up a second manufacturing facility to build buses. Usually this type of growth is fairly easy for the IT department to deal with. The scale of the operation may increase, but the basic issues of how to manage the IT department do not change. From a security perspective, you may be faced with the additional complexity of having to deal with information flowing among multiple locations, but in general the security issues will not change.

A third way that a corporation can grow is to start up new companies in new business areas where the corporation has not worked previously. In many cases, the new company is closely linked to a business that the corporation is already involved with. For example, an insurance company may start a real estate management company so it can buy and directly manage the commercial buildings the insurance company is buying with its customer's premiums. In other cases, the new company may be a significant departure from what the company has done up to that point. The bus manufacturing company may decide to start an online company selling pet food. A corporation that grows by starting up a new business can create some interesting challenges for the IT management. Although you may be working with the same people and policies in the new company, you may be faced with a variety of new challenges. From a security perspective, you may be facing a whole new set of issues in the new company. You may understand the security risks in the parent company, but if the new company is branching off into a new business area, you will first have to learn the security issues in the new field.

In order for you to create a good security plan, it is essential that you take into account how the corporation plans to grow. In some cases, this information may be confidential and you may not be given the necessary information for fear of what might happen if the information is released prematurely. Even if you are not given information on specific options the company is working on, you do need to at least understand, in broad terms, where the company is going. You can also look at the corporation's history to gain an understanding of how the company grows. In most cases, a corporation will follow a consistent pattern of planning for growth.

Closely tied to corporate growth strategies is the corporation's tolerance of risk. This book deals with how to manage security risks from an IT perspective, but the company also has a tolerance for risk from a business perspective. This tolerance for risk usually appears most clearly in the corporate growth strategies. A corporation with a high tolerance for risk is characterized by aggressive mergers and acquisitions, or frequent start-ups of new companies. A corporation that has a low tolerance for risk is more likely to try to grow by expanding the current business, or by acquiring or starting businesses that are similar to or integrated with the current business. A company with a high tolerance for risk may be an interesting place to work because things are constantly changing, but this constant change also introduces serious security-related issues. A company that is constantly taking on new risks may also inadvertently open security loopholes that someone may exploit. If you are working for a company with a high tolerance for business risk, your security plan will need to clearly define a rapid modification and deployment procedure for the security policies. Your security plan modifications will have to keep up with the corporate changes. A corporation with a low tolerance for risk probably will change its security policy slowly and infrequently. The biggest challenge in this company might be coming up with a security policy that matches the corporate policy and eliminates all security risks to a maximum degree. In this company, you may have time to develop a thorough security plan, but you will also have to deal with every possible security risk.

Integration with IT

As you examine the corporate growth strategies, you also need to examine how those strategies are integrated with the IT infrastructure. Almost every company depends on the IT infrastructure to get its work done, and the corporate growth strategies need to allow for this fact. The IT infrastructure is a core component of almost any corporate plan for growth. In some cases, IT innovation can even create new opportunities. A common example in today's economy is the use of the Internet. Most corporations see the Internet as an opportunity to reach new markets and to make it easier for customers to contact them. Companies use the Internet to provide sales information, but also to support a product after it has been sold. An IT staff that is aware of the business possibilities of using a technology such as the Internet may be able to help the corporation grow rapidly.

Making maximum use of IT to achieve corporate goals requires a good working relationship between the IT staff and upper management. Virtually every business effort now depends on information technology, and nobody understands the technology better than the IT professionals. If the IT staff also understands where the company is going and how it plans to get there, they can design all IT projects to help the corporation take advantage of the opportunities for growth.

Identifying IT Administrative Structures

After you have identified the business issues that will affect your security plan, you are ready to move on to gathering information about the IT infrastructure at your company. To begin with, you will again be doing a fairly high-level analysis of how the IT department is managed before moving on to collect information about the more detailed specifics of the day-to-day network and security management.

There are three models of network administration that are similar to the models of corporate management discussed earlier. The first model is a highly centralized IT management. In a centralized model, all of the network management is performed by one person or small group of people. This is a typical model in many medium-sized businesses. For example, a company may have several thousand users, most of whom are located at a corporate head office with several small branch offices. Often the central IT team at headquarters performs all of the network administrative tasks. Sometimes all of the network services, such as the corporate messaging servers and database servers, are also located in the central office. Most often these organizations will have a single domain, and, if they are running Active Directory, they might have a separate organizational unit (OU) for each remote location.

The second IT administration model is a decentralized or distributed model. In this case, the network administration tasks and the network services are distributed throughout the organization. This is the model typically followed by large corporations with multiple locations and thousands of users in each location. Another common scenario where you will find a decentralized administrative model is in a corporation that has merged with, or acquired, other companies, and each company remains fairly autonomous. In this model, each location or business unit does most of its own network administration. Often each location has a separate Windows NT or Active Directory domain so that the security boundaries between locations are also enforced by the directory services boundary.

The third IT administration model, and the most popular model in medium-to-large corporations, is a hybrid model. In this scenario, some aspects of network administration may be highly centralized while other components are decentralized. A common example of this model is a corporation that gives considerable authority to each location or business unit to manage their own network, while centralizing some services. Often services such as e-mail, or WAN management, are centralized with a single team at the company head office. The reason for the centralization may be that the service requires

a special skill set (such as managing the corporate Exchange servers) or because the service overlaps to all locations (such as managing the WAN connectivity). One of the biggest advantages of Windows 2000 Active Directory over Windows NT is the way it supports a hybrid network management model. With Active Directory, you can create a domain and OU structure where a group of administrators at each remote office can have almost complete administrative control over the local administrative tasks, such as managing users and computers, while still allowing a central administrative team to manage the network services that affect all of the locations.

A fourth network administration model that is used by some corporations is an outsourcing model. In this model, the corporation hires an external IT firm to manage some or all components of the network. The actual components that are outsourced vary a great deal. If a corporation needs access to a mainframe system, the management of the mainframe system may be outsourced. Sometimes specific components like web server management or the e-mail servers are outsourced, while the user and group management, and the other network services are kept in-house. Sometimes the outsourcing is more temporary and project based. The corporation may outsource the migration of the Windows NT domains to Windows 2000 Active Directory, but retain complete administrative control of the network after the migration.

The IT administrative model used by your company has serious implications for your security planning. In general, the security model should be one of the most centralized components. If the corporation has a decentralized-network administrative model, and the security planning is also decentralized, you can encounter some interesting problems. For example, if each location is managing its own firewall configuration, the corporation may find itself supporting multiple firewalls. Even if all the firewalls are the same, they may be configured differently so that you may have some ports open in some locations and closed in others. If the security planning is decentralized, you may find out that the locations have incompatible security requirements. For example, one office may decide that they need a password policy that forces password changes every 30 days, while another office may want password changes only every 60 days. If both offices are in the same domain, there is no way to satisfy both requirements. For these reasons, it is usually preferable that at least the design for the security policy be centralized, and one security policy created for the entire organization. Even if different locations have different security requirements, centralizing the planning can ensure that the locations are not developing incompatible security policies.

Identifying the Current Technical Environment

After identifying the top-level administrative model for the corporation, the next step is to begin gathering more detailed information about the IT infrastructure. One of the basic concepts of any kind of IT planning, including developing a security plan, is that you can never have too much information. You will want to know everything you can about the current network configuration before embarking on your design project.

As you work with a variety of companies, you will find out that they vary greatly in the documentation they have about their own infrastructure. Some companies have excellent documentation and can quickly provide you with the detailed information that you need about their networks. More common are the companies whose network documentation is badly out of date, or where some components are completely missing. As you begin to collect information about the network, be prepared to do a great deal of research in order to come up with the information needed.

Corporate Locations

As you begin collecting information, you will have to research the company locations. A company may have only one location, two locations in the same city, or it may have multiple locations scattered throughout the world. For each location, you need to collect the following information:

- Geographic locations—Where are the corporate locations? Are they all located in the same region of a country, in the same country, or in several countries around the world? Are the locations all in big cities with an excellent WAN infrastructure, or are some locations in smaller centers with very few options for WAN connectivity?
- Business Units at each location—What business units are located in each of the geographic locations? To what extent do the geographic locations correspond to business units? In some cases, each geographic unit may have only a single business unit; in other cases, some members from each business unit may be located in every location.
- Number of users at each location—How many users are there in each location? This listing of users should include the total number of users, as well as some indication of the functions performed by the users. A manufacturing location with 1,000 workers who use the computers to access only e-mail and an AutoCAD application will have very different security requirements from a research and development location where all of the users are using computers to do top-secret research.
- Number of remote users—An important consideration for designing a security plan is the number of remote users, or users outside the company location, who need access to resources on the corporate network. Providing network access to remote users is one of the biggest security issues that you will need to deal with, so an accurate count of the number of users at each location and knowledge of what resources on the network they need to access will be essential.

Networking Infrastructure

After you have gathered the basic information about each location, you need to gather more detailed information about the network infrastructure at each location. The information that you need to collect includes:

- The physical network topology at each location, including the LAN configurations, hub or switch configurations, and backbone topology. Usually this information is provided in the form of a network topology diagram and includes all of the server connections at each location. Figure 2-5 is a sample illustration of a simple network topology diagram.

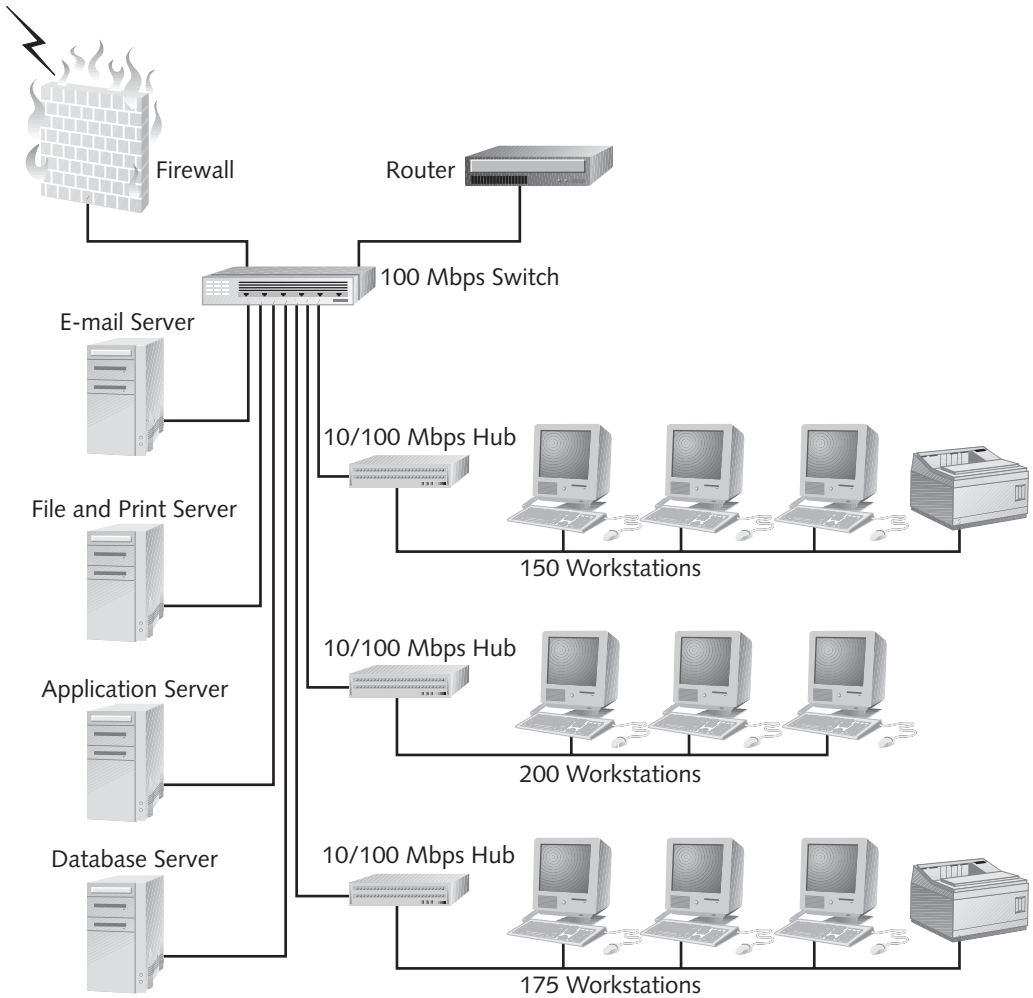

Figure 2-5 A sample local area network diagram

- The WAN topology, including a diagram of the WAN topology, total bandwidth, available bandwidth, and router configurations. The WAN topology will be essential in creating the security plan because many of the security issues that you need to deal with relate to protecting traffic on the WAN links, especially if the Internet is used to connect corporate locations. Figure 2-6 shows an example of the information in a WAN topology diagram.

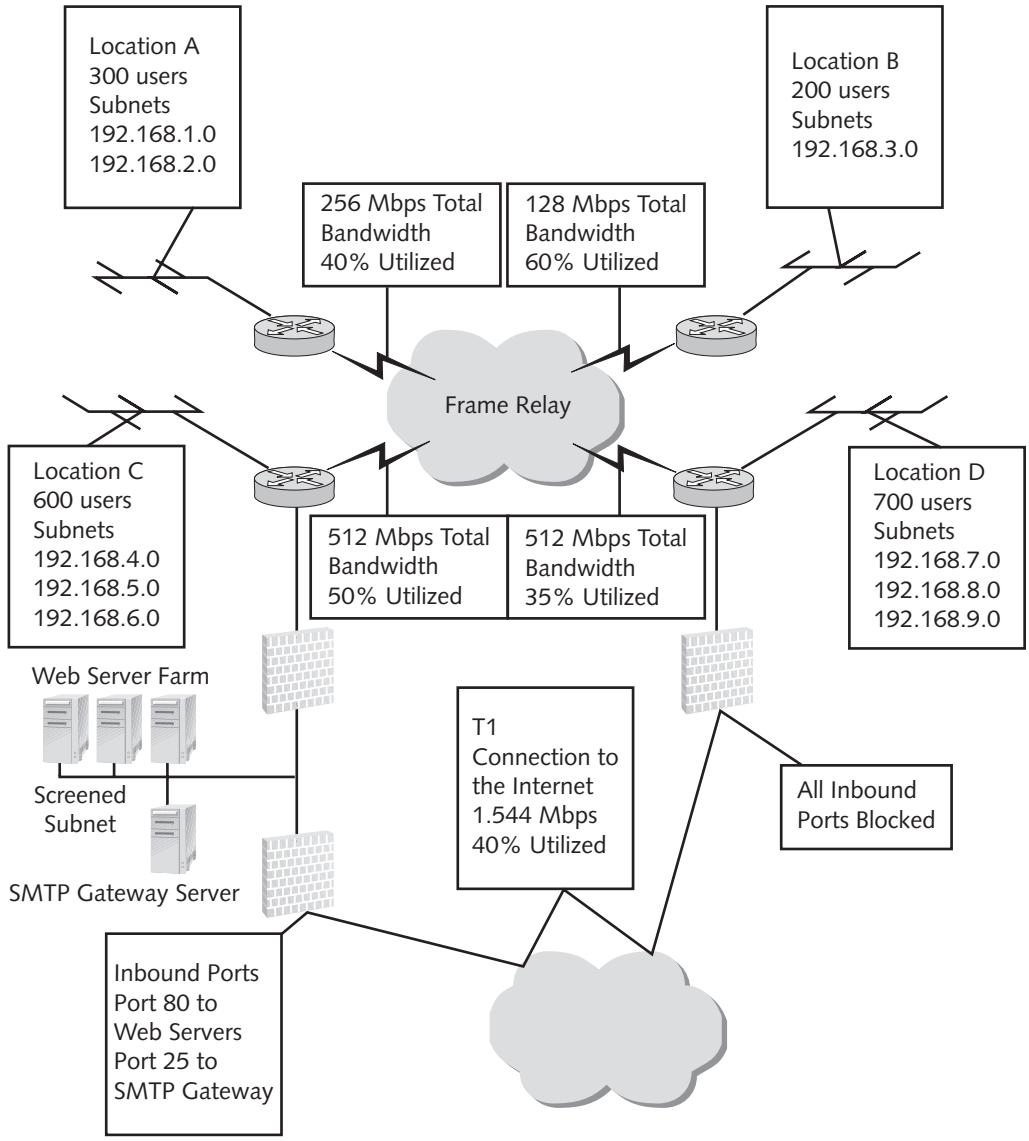

Figure 2-6 A sample wide area network diagram

- The Internet access points where your network connects to the Internet. Your security plan must protect these crucial points. For each point, you need to know the network connectivity (total and available bandwidth), the type of connection, and the firewall and proxy server configuration. Some of the information that you need to gather is shown in Figure 2-6.
- The remote access configuration, including RAS servers and dial-in and VPN configurations.
- The protocols supported at each location. This should include the addressing information. For example, if TCP/IP is used at a corporate location, you need to collect information on the IP addresses that are assigned in each location, as well as the routing table configuration.

Networking Services

After you have gathered the basic network infrastructure information, you also need to gather information about the networking services at each corporate location. The networking services information that you gather should include:

- The Dynamic Host Configuration Protocol (DHCP)—This is an extension of the TCP/IP information that you need to gather for each location. DHCP is used to automatically assign IP configurations to client computers.
- The Windows Internet Naming Service (WINS), and Domain Naming Service (DNS) configurations—Both of these services provide name resolution services, with WINS used for pre-Windows 2000 servers and clients, and DNS for Windows 2000. In addition to the internal DNS configuration, you also need to gather information about the DNS information that your corporation makes available on the Internet.
- Network services—Every corporation runs a variety of network services. Almost every company has an e-mail infrastructure; most companies have business applications that use a database server as a backend. Many companies have also deployed web servers, both for Intranet and Internet web sites. Some companies have also invested in terminal servers, where many of the business applications are running on a terminal server with the client computer connecting using a thin client. These services are mission-critical in most organizations; if one of the services shuts down, the business productivity can be seriously affected. Because of this, your security plan has to include ways to protect these services.

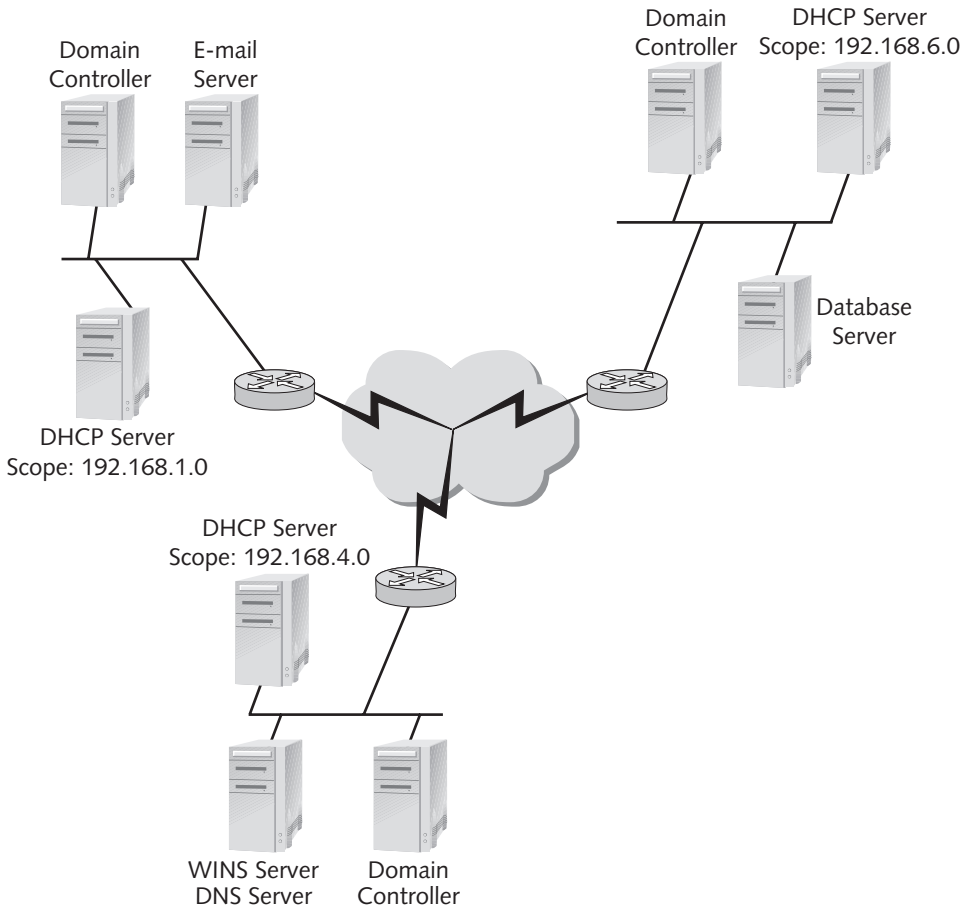

Figure 2-7 Information you should gather about networking services

Network Administration

You will also need to collect information about how the network is administered in your organization. This information includes any documented procedures for how network tasks are performed, as well as an outline of who is responsible for each task as follows:

- User and group administration, including who is responsible for creating, deleting, and modifying user accounts, and whether there is a standard procedure for the process.
- Regular administrative tasks, such as information on backup procedures, restore procedures, anti-virus software implementation, monitoring activities, and who is responsible for performing these tasks.

- The network administration and support management procedures, including who is responsible for monitoring and managing the network infrastructure and the current management strategies.
- Troubleshooting procedures, including how troubleshooting issues are dealt with, what the different levels of support are, and whether there is a clearly defined process for quickly resolving a troubleshooting issue.
- Disaster recovery procedures, including what plans are in place to recover from a disaster, who is responsible for keeping the procedures up-to-date, and when the procedures were last reviewed and tested.

Configuration Change Management

Closely linked to the current network administration procedures are the procedures the company uses to change the configuration of the network or to adopt new technologies. Information that you should gather in this area includes the following:

- Does the corporation have a clear change-control mechanism in place? What procedure is used to initiate, test, pilot, and implement changes to the network?
- What is the user reaction to the change-control policy? In some companies, the change-control policy is so convoluted and time-consuming that users are constantly trying to circumvent the policy because they think that it is preventing them from responding to urgent business needs.
- Is the change-control procedure proactive or reactive? Some proactive companies have dedicated IT staff who are constantly testing and evaluating new technologies to see how new technologies can help the business. More frequently, however, new technologies are only evaluated when a business unit requests the new functionality.
- How are network administrators and end users informed of configuration changes? In the case of major changes, are the appropriate people trained in how to use and support the technology?
- How does the corporation deal with changes that involve ongoing maintenance? For example, Microsoft frequently releases hot fixes for its operating systems, and usually at least two service packs a year. How are the service packs tested in the corporation? How are they implemented?

Client Requirements

The final category of information that you need to collect involves client requirements. The list of requirements that a normal user needs to be effective on the job should include the following:

- What operating systems are supported on client computers? Are there any applications that require a particular operating system?

- Is there a standard desktop configuration for the client computers? If there is, what is included in the configuration? Typically, this configuration includes a standard set of office applications, a web browser, and an e-mail client, as well as any special clients for custom business applications.
- Does every user get their own computer that they use all the time? Or do users share computers? Do users move between many different computers? Does the corporation support roaming user profiles?
- How are the client computers managed? Are users allowed to store data on their local hard disk? Does the corporation use disk-cloning software to rebuild computers? Are system policies or group policies used to manage user desktops?
- What resources do the users need to access? In most companies, everyone gets access to e-mail, but only some users may get access to the Internet. Every client probably needs access to the corporate file and print servers. Is there a standard configuration for how the clients access these resources? For example, is there a standard set of mapped drives assigned to all users in a department?
- What are the performance expectations for the clients? The clients probably have many performance expectations, including how long it should take to copy a file onto a network share, how long it should take for an e-mail message to go from one user to another, and how fast the Internet connection should be. Document the expectations and where those expectations are being met, but also document the constraints. Why does the corporation not provide the performance that the clients would like? Often the crucial issue is the cost of providing the level of performance requested by the clients.
- How do users get the authentication needed to access network resources? Is there a single logon procedure that gives users access to all network resources, or does the user have to log on repeatedly to get access to different resources? In many organizations, users have to enter their user name and password when they first log on to the network, when they go through the firewall or proxy to access the Internet, and when they access an application running on a Unix or mainframe server. How are the user accounts and passwords synchronized across the multiple logons?
- How is the remote client configuration different from the local client configuration? Is there a standard configuration for laptop computers? How do the remote users get access to the network resources?
- What additional devices do the clients use? Many users now have wireless devices for checking e-mail or surfing the Internet. Web-enabled phones can be used to check e-mail on some corporate e-mail servers. Personal Digital Assistants (PDA) have become a standard part of the desktop for many executives or people who spend a significant amount of time out of the office. When collecting this information, also gather information on what types of devices the corporation provides support for, and what types of devices are permitted, but not supported.

Identifying the Current Security Model

After collecting all of the related information about the business and the current IT infrastructure, you are finally ready to move on to analyzing the current security model. This is a prerequisite to creating a new security model, just as the other types of information discussed in this chapter have been prerequisites. Before you can begin to plan a new security policy, you need to understand the one that is already in place. Understanding what is already in place can be very useful in at least two ways. By looking at the current policies, you get a good indication of what needs to be changed. At the same time, you may find many aspects of the current policy that work well and do not need to be changed.

Physical Security

To begin, take a look at the physical security configuration for the corporation. There are a number of questions that you need to ask at this point:

- Are the servers locked in a server room? Many security holes in Windows 2000 can be exploited only if the attacker can get physical access to the server, so locking up the servers is a crucial first step in a security policy. If the servers are locked up, who has access to the server room? How is that access controlled? Is access to the server room logged?
- How are the servers administered from outside the server room? Most network administrators do their work from workstations at their desks, so how are those workstations protected? Is there a policy of locking the workstations whenever the administrators are not at their desks? Do the administrators use password-enabled screen savers? Do the administrators always log on with their administrator accounts or do they use these accounts only to perform administrative tasks?
- How is physical access to the network handled? One of the worst possible security breaches occurs when someone runs a packet sniffer and captures all of the traffic on your network, so how do you protect against this? Does the corporation require security passes for access to any locations where an intruder might get access to the network? What is the corporate policy on outside consultants bringing in laptop computers? Are the consultants allowed to connect their computers to the network, or does the company provide each consultant with a desktop computer?
- How is access to network devices controlled? Are the network hubs, switches, and routers locked in a wiring closet or in the server room?
- How is the physical security of corporate laptop computers handled? Laptops are often used by corporate executives who may be storing confidential information on the laptop hard disks. The theft of the laptop could mean the

theft of the data. Are the laptops equipped with a lockable cable to make the theft of the computer more difficult? Does the corporation have policies about where the laptop can be taken and where it can be left unattended? What operating systems are supported on the laptops?

- How are printers that print confidential documents secured?

Network Security

In addition to information about the physical security of the network, there is a great deal of network security information that you need to gather before developing the security plan. The entire list of what you need to collect is very long, and as you go through the rest of this book you will learn a great deal about the information that would be included in a security plan. The following short list is a sample of what you need to collect:

- The Windows NT domain configuration (including trusts), or, if the network has been migrated to Windows 2000, the Active Directory configuration—If the organization is running Active Directory, you also need to collect information on the OU configurations and the group policies used to set security and desktop configuration options for each OU.
- The password policies in the organization—How often do passwords need to be changed? What lockout policy is in place for when users try to logon repeatedly with the wrong password? What are the password length and complexity requirements? Who has the right to reset user passwords?
- The types of network or web applications used on the network—Do any applications require basic authentication, in which the password is sent across the network in clear text?
- Firewall and proxy server configurations—How is security configured on the file shares on the servers? Are share permissions or NTFS security used? Who is responsible for managing the permissions on the shares?
- A Public Key Infrastructure (PKI)—If the corporation uses one, does it use a Windows 2000 Certificate Server or certificates from a public certificate authority? What is the PKI used for: secure web sites, secure e-mail, encrypted file system, IPSec?
- VPN and RAS server configuration—Who is allowed to connect to the network remotely? Are remote access policies used to control access to the network? What authentication protocols are used?
- Current security audit requirements—How is auditing configured, and who is responsible for monitoring the audit logs?

As you document the security settings that are currently in place, you should also document who is responsible for setting the policy and who is responsible for administering the security policies. Most large organizations have a designated security officer who is responsible for setting the overall policies and providing the documentation on how the policies should be implemented. In smaller organizations, the role of security officer is usually assigned to one of the network administrators, or left as a responsibility for the entire team. In addition to knowing who sets the security policy, you also need to document who actually administers the security policy, and what procedures are provided to implement the policy.

Obviously, this is just some of the information that you need to collect as you begin your security planning. Collecting all the required information can be a lengthy task, but it is a crucial step in designing a security plan. Some corporations may already have all of these security settings documented; others have virtually no documentation and the security policy has been developed in an ad hoc manner. As you go through this book, and as you explore options for securing your network, you should ask how each particular issue is being handled now, and whether the current policy needs to change.

Chapter Summary

- The business model adopted by a corporation can greatly affect the corporate security plan. Business model components include the ownership of the corporation, the company's products and services, the corporate business processes, the corporate management structure, the geographic scope, and business relationships with other corporations.
- The corporate goals and strategies also have a great deal of influence on the corporate security plan. The corporate vision and goals define the corporate direction. Frequently, the corporate goals include growth strategies, which can involve acquiring other companies, starting up new business units, or expanding the current business units. In designing a security plan, you have to look at the future of the organization to ensure that your plan meets the future needs of the corporation.
- Every corporation has an IT administrative structure that frequently follows the corporate management structure. A corporation with a hierarchical and centralized corporate structure is likely to have a centralized IT administrative structure. The IT administrative structure can have important implications for the security plan. In general, it is preferable to have the corporate security plan designed and implemented in a centralized model so that all business components have compatible policies.
- After gathering the business information and determining the IT administrative structure, you can begin to gather detailed information about the current IT infrastructure. The information that you need to gather includes information about the corporate locations, the networking infrastructure, including the LAN and WAN configurations, the networking services, and the client requirements. Your security plan will need to protect all of these resources, so you need extensive information on the current IT infrastructure.

- Before developing a new security plan, you also need to gather information on the current IT security plan. In most cases, your security plan will build on what already exists; you will not change the components that provide the required security, and you will enhance the components where more security is needed.

Review Questions

1. In a publicly owned corporation, the role of the board of directors is to:
   a. own the corporation
   b. directly manage the day-to-day operations of the corporation
   c. hire the executive officers to manage the corporation
   d. represent the corporations' owners in setting corporate direction
2. The primary goal of most public corporations is to make money for the corporation's owners. How can this affect the security planning for the corporation?
   a. It should not have any effect.
   b. If the corporation is losing money, the security projects are more likely to be cancelled.
   c. Security projects that can be shown to increase corporate profits are more likely to be approved.
   d. The budget for security-related projects is likely to be very small.
3. If you are working for a corporation that has a history of stability and growth, your security planning is likely to be focused on:
   a. short-term projects
   b. only the most important security issues
   c. the least expensive projects
   d. addressing longer-term issues
4. A corporation that is a wholly owned subsidiary of another corporation is likely to:
   a. have some restrictions set on its business practices by the parent company
   b. be able to operate as a completely independent business entity
   c. have all business decisions made by the parent company
   d. have a great deal of influence on the business practices at the parent company
5. Understanding your corporation's business processes will help you to develop a better security plan because:
   a. You will understand how the applications work that are used by the business users.
   b. You will understand the security risks at each step in the process.
   c. You will understand how much money the corporation is making.
   d. Each step in the process will represent an additional security risk.

6. A company that provides financial services is likely to have different security requirements than a company that manufactures windows because:
   a. The value of the company is much higher.
   b. The security infrastructure is not as elaborate.
   c. The potential risk is much higher.
   d. The company is easier to attack.
7. Many corporations are now making a great deal of information available on their web sites to customers and partner organizations. How does this make the security planning more complex?
   a. You may have to provide many different levels of access on one web site.
   b. It doesn't make the security planning more complex.
   c. You can't ensure that the web site is secure.
   d. The web site is susceptible to denial-of-service attacks.
8. The security plan for a corporation with multiple locations is likely to be more complex than the security plan for a corporation with a single location because:
   a. The company will always have more than one domain.
   b. The company will have many more users.
   c. The traffic on the connections between the locations will need to be protected.
   d. The security plan will have to address the physical security in more than one location.
9. A corporation with a highly centralized management model is likely to have:
   a. a powerful CEO that is directly involved in the important decisions
   b. a strong emphasis on everyone contributing to the decision making
   c. strong management teams that share decision making
   d. a non-hierarchical structure
10. If your company has adopted a decentralized management structure, your security planning may be complicated by:
    a. the slowness of the decision-making process
    b. the difficulty in implementing one corporate standard in all locations
    c. a lack of money for designing your security plan
    d. the power of the CEO to dictate all decisions
11. If different business units in your corporation develop their own security plans without reference to a corporate standard, the security plan is likely to be more complicated and difficult to implement. True or False?

12. When a corporation forms a partnership with another corporation, the security planning is more complicated because:
    a. More people will be included in the security plan.
    b. You will have to create a trust between the two organizations.
    c. You will have to manage the other corporation's security plan as well.
    d. You do not have control over the other organization's security, which might put any data you share with them at risk.
13. When your corporation acquires another corporation, you are told that the two IT infrastructures will be merged. Your first step in redesigning the security plan should be:
    a. informing the other company of your corporate security standards
    b. enforcing a consistent password policy across the entire organization
    c. investigating the current security plan in the other organization
    d. ensuring that the two security plans do not overlap with each other.
14. Your company has made a commitment to grow rapidly by expanding the current business practices rather than moving into different business areas. You think that you have an effective security plan in place. How will the rapid expansion affect your security plan?
    a. It is likely to have little effect.
    b. You will have to redesign your entire security plan.
    c. You will have to include many new issues in your security plan.
    d. The security plan is likely to become less complicated.
15. The advantages of having centralized IT administrative structure are:
    a. More administrators will be required.
    b. It is easier to adopt and enforce one corporate standard.
    c. The cost of managing the network will be significantly reduced.
    d. You may be able to reduce the number of servers in the organization.
16. When a company decides to hire another company to manage its IT infrastructure, the company has adopted an _____ model of IT administration.
    a. outsourcing
    b. centralized
    c. de-centralized
    d. vendor

17. Accurate information about users who access the corporate network through remote access is important when designing the security plan because:
    a. It is costly to provide laptop computers for the remote users.
    b. It is difficult to obtain the required information.
    c. Remote users present a security risk.
    d. Many remote users are likely to be the corporate executives.
18. As you design your security plan, accurate information about the WAN connections within the company is important because:
    a. The WAN connections are the slowest part of the network.
    b. The WAN connections expose information to the Internet.
    c. The cost of the WAN connections is high.
    d. You must make sure that the data on the WAN connections is secure.

HANDS-ON PROJECTS

Project 2-1

In this hands-on project, you will conduct research on a specific company in order to understand various concepts to assist in the design of a security plan.

To access the company web site:

1. Log on to your Windows 2000 computer as an administrator.
2. Open Internet Explorer by double-clicking the **Internet Explorer** icon on the desktop or in the taskbar.
3. In the Address Bar, type **www.microsoft.com/technet**. This will take you to Microsoft's Technet web site.
4. On the Technet web site, click in the search box and type **Rhode Island College**. Click the **Go** button to search for the site.
5. In the results pane, click the link that states **Rhode Island College uses Windows 2000 Security…**
6. To gather information regarding Rhode Island College, read the Rhode Island College case study and answer the questions that follow.

   To evaluate the security needs of Rhode Island College:

   a. What types of business does Rhode Island College engage in?
   b. What types of data have to be protected within the college network?
   c. What are the main security challenges facing Rhode Island College? How likely are these threats?
   d. How did the consultants overcome the security challenges listed? Is there anything that you could do to add to the security of the network?
7. Close Internet Explorer.

Project 2-2

In this hands-on project you will prepare a report to assist Rhode Island College in their security plan.

1. Rhode Island College wants you to write a report to explain the various types of IT Administrative models that can be implemented within Windows 2000 Active Directory. List four administrative IT models and the security implications of each. (*Hint*: Consult chapter 2 of the MCSE Guide for information.)

   a.

   b.

   c.

   d.

2. Rhode Island College needs your advice regarding an effective password policy. Write a short paragraph expressing your views and outlining best practices regarding password length, complexity, who creates and maintains the passwords (administrators or users), and the practice of forcing the changing of passwords.

Project 2-3

In this hands-on project, you will conduct research on a specific company in order to understand various concepts to assist in the design of a security plan.

To access the company web site:

1. Log on to your Windows 2000 computer as an administrator.
2. Open Internet Explorer by double-clicking the **Internet Explorer** icon on the desktop or in the taskbar.
3. In the Address Bar, type **www.microsoft.com/technet**. This will take you to Microsoft's Technet web site.
4. On the Technet web site, click in the search box and type **Orange County**. Click the **Go** button to search for the site.
5. In the results pane, click the link that states **Orange County, Florida, Schools Use Security Features In Windows 2000 for Decentralized Control, VPNs**.
6. To gather information regarding the Orange County case study, read the Orange County case study and answer the questions that follow.

   To evaluate the security needs of Orange County:

   a. What types of data have to be protected within the Orange County/Florida network?

   b. What are the main security challenges facing the school? How likely are these threats?

c. How did the consultants overcome the security challenges listed? Is there anything that you could do to add to the security of the network?

d. How is the school addressing the need for security between the WAN links?

e. What other general security issues arise when planning security for a national or international WAN connection?

7. Close Internet Explorer.

CASE PROJECTS

Technical Consultants is a large multi-national IT consulting company with 30 locations throughout the world. Technical Consultants provides a wide variety of IT consulting services, including mainframe support, application development, and infrastructure planning and deployment to other large corporations.

The corporate headquarters are located in Austin, Texas with approximately 20,000 employees at head office. Each of the thirty locations has from 50 to 3,000 employees. In addition, the corporation has many consultants working on site at customer locations. There could be up to 30,000 consultants working at a maximum of 2,500 customer locations. Many of the corporate executives and sales people travel extensively throughout the world.

All employees, including the traveling users and consultants on client sites, must be able to access the corporate network. All of the users must be able to access the corporate e-mail servers through a web interface, as well as gain access to potentially confidential information through the corporate Intranet site. In addition, many users require access to files and applications that are located on the corporate network.

The corporate locations are connected to head office and to other corporate locations through a variety of dedicated WAN links. Each of the corporate locations also has a direct connection to the Internet. Most of the users who are working on client sites can use the client corporation's Internet connection, although some users, including many of the traveling users, are still using a dial-up connection.

The corporation has completed the deployment to Windows 2000 Active Directory and is currently configured as a single Active Directory forest with a single dedicated root domain with 12 child domains, one domain for each country where the company has a location.

1. What are the most important security concerns that Technical Consulting will need to be concerned about?
2. How are the security risks for a large multinational corporation like Technical Consulting different from the security risks for a smaller company like Southdale Property Management or Fleetwood Credit Union?